New Mexico Municipal Court Automation
Guide to Disaster Recovery Planning

June 2007

New Mexico Municipal Courts Automation Program
Zella Cox, Program Manager
(505) 476-6943 | zellacox@nmcourts.gov

Tomás Aguirre, Database Administrator
(505) 476-6962 | taguirre@nmcourts.gov

April Sessions, Information Technology Specialist
(505) 476-6967 | asessions@nmcourts.gov

Table of Contents

New Mexico Municipal Court Automation
Guide to Disaster Recovery Planning

I. Introduction

Disaster recovery is the process of restoring business operations after a disaster or other unplanned event causes disruption of normal business operations. Disaster recovery planning is the process of evaluating scenarios and documenting the steps needed to restore operations after a disaster. A Disaster Recovery Plan (DRP) is often part of a larger process known as a Business Continuity Planning (BCP) and may be a subset of a court's or a municipality's Continuity of Operations Plan (COOP). Because we depend on automated systems for most of our day-to-day work, protection and restoration of these systems will comprise the bulk of the DRP.

This document introduces some of the key concepts used in disaster recovery planning and provides a starting point for thinking about how your court would deal with a disaster that destroyed or disabled your automated systems. Courts face unique challenges in responding to disasters, large and small. Since court business is time sensitive, with deadlines set by rules and statutes, delays must be minimized. Because court records are extensive and critical, these records must be protected. Courts must provide leadership and remain responsive to the communities they serve, even in the face of disaster. Therefore, it is imperative that courts develop contingency plans for events that might disrupt the normal flow of business.

Disaster planning is not a one-size-fits-all process, as each organization must assess its own risk factors and critical functions, as well as its tolerance for risk. All of these items must, of course, be balanced by funding considerations. In some industries, it is common to spend up to 25% of a company’s budget on disaster recovery planning. This expense is justified because it helps to avoid larger losses. Of companies that have experienced a major loss of computerized records, 43% never reopen, 51% close within two years, and only 6% will survive long-term (Cummings, Haag & McCubbrey 2005). Public organizations are in a unique position because they are often holders of public records and have an obligation to the community. While one cannot plan for every possible contingency, we can take reasonable steps to mitigate damage from the most likely events.

Once a Disaster Recovery Plan is in place, the court must ensure that copies of the plan are readily available. Copies of the plan should be maintained on paper and electronic media in a safe, yet accessible, location. Review the plan frequently so that changes in equipment, personnel, and procedures can be documented. Provide opportunities for practice runs on critical procedures, and ensure that the disaster recovery procedures are covered in all new employee orientations. Ensure that personnel are familiar with the plan and their responsibilities and that they have all necessary training.

II. Events That Necessitate Disaster Recovery

Many different events can negatively impact the normal operations of an organization. Even a simple (and relatively common) power outage can cause undue disruption and delays by making forms and schedules inaccessible. A risk assessment should be performed to determine the risks to which an organization is susceptible. The list of possible disasters is endless, but this list can be narrowed down depending on a court's geographical location and other factors. The following are some events to consider for a DRP:

- Fire
- Floods and other water damage
- Hurricane, tornado, or earthquake
- Power failure
- Equipment failure
- Bomb threats or other forms of terrorism
- Sabotage
- Theft
- Human error
- Computer viruses, worms, and other intrusions
- Impoundment or confiscation of equipment
- Unexpected loss of contracted services
- Temporary or permanent loss of key personnel

III. Disaster Recovery Planning

The primary goal of disaster recovery is to restore essential business functions as soon as possible. A DRP provides the specific steps needed to ensure an orderly restoration process.

The planning process consists of the following steps:

1. Assess business impact and risk: it may be useful to plan for worst-case scenarios, because plans can always be adjusted downward for lesser disasters.

    A. Define and document the court's essential functions

    B. Define and document likely risks

    C. Evaluate each possible scenario in terms of consequences, desired outcome, and necessary actions

2. Define short and long term objectives of disaster recovery

    A. Short term objectives may include restoring essential services within a certain number of days or hours. Depending on the cause of the disruption, this may be as simple as recovering back-ups from tape or other backup storage, or as complex as replacing

entire systems. Short-term relocation may be necessary, in which case a laptop computer becomes an invaluable asset. Consider alternate (i.e., old-fashioned) methods of accomplishing time-critical tasks in the event of a total loss of automation capability.

B. Long term objectives may include permanent relocation of personnel and facilities, replacement of equipment and furnishings, and recovery/restoration of archival data. A worst-case scenario might include coordination with the City Attorney, law enforcement, and other municipal offices to rebuild critical data files.

3. State assumptions of the plan

A. Define what will be considered a disaster.

B. Determine if the plan will cover only worst-case disasters, or if it will cover lesser disruptions as well.

C. State what types of controls are assumed to be in place, including backup systems and smoke/fire alarms/other early warning systems.

4. Define the organizational structure

A. Identify a team leader and an alternate plus other key personnel. Outline the chain of command, including alternates for all key positions. An organizational chart will clarify the chain of command and help everyone understand their roles in the recovery effort.

B. Identify means of obtaining additional help if regular staff are unavailable, including contact numbers and cost/payment details for contract labor.

5. Define the communications structure

A. Communication is critical during any disaster, as well as during the recovery and follow-up phases. Consider that you might not have access to automated systems, and develop contingency plans for notifying affected parties of delays or relocation:

- Judges and alternate judges
- Court administrators and clerks
- IT staff and consultants
- Contract or temporary employees
- Plaintiffs and defendants, witnesses, attorneys, law enforcement, and any other parties that could be affected by delays

B. Identify authorities that will need to be notified in the event of a disaster, from the mayor or council members up to state government and congressional representatives.

C. Help minimize panic and disorder by notifying the public about a problem and the steps being taken to solve it.

- Identify contacts for public announcements (radio, TV)
- Identify supplies needed to make signs notifying the public of delays and relocation.

D. Keep a current list of vendor contacts in the event their assistance is needed to restore data or applications.

E. Larger organizations may want to consider setting up phone trees to notify personnel of procedures and assignments.

F. Identify alternate forms of communication, such as 2-way radios, in the event that regular communication channels are unavailable. A "sneaker-net" may be needed to carry applications and data from a disaster site to a temporary facility.

Contact information can include landline and cell phones, email and alternate email addresses, and in some cases, physical location.

6. Inventory equipment and software

- Record models and serial numbers
- Record monetary values and place of purchase/vendor details
- Secure photographs of major equipment
- Protect warranty and instruction manuals
- Identify replacement sources for equipment and anticipated wait times for repair or replacement
- Define acceptable downtimes
- Define priorities for equipment repair and/or replacement
- Identify funding sources for equipment repair and/or replacement
- Maintain and document vendor maintenance contracts for critical systems

7. Define data storage and backup requirements

A. Information systems must include backup capabilities to limit data loss and aid data recovery. First, one must identify what types of data need to be stored and develop a framework for storage and recovery of the data. All data types should be analyzed to determine an appropriate back up strategy for each. The following metrics are commonly used to determine the frequency and priority for backups. This, in turn, will help you determine what type of backup system you need to use. The closer an application’s Recovery Point Objective (RPO) and Recovery Time Objective (RTO) values are to zero, the greater the organization’s dependence on that particular process, and consequently the higher the priority when recovering the application after a disaster.

- Recovery Point Objective (RPO) quantifies how current restored data has to be. The RPO denotes the amount of data an application can lose before an organization begins to suffer. This, in turn, helps determine how frequently backups will need to be made. A court that handles hundreds of cases in a day might measure the RPO in hours. In a smaller court, it may be measured in days. The RPO helps you think about how much data you are willing to lose, and therefore have to re-enter or re-create, in the event of a loss.

- Recovery Time Objective (RTO) indicates how much time can elapse before data is restored, and therefore, how long the IT staff will have to bring an application back online after a disaster. It may be measured anywhere from minutes to days or weeks depending on the type of data. Different values may be assigned for different types of records, and they will vary widely among current records (open/active cases), historical records (cases that are within regular retention guidelines), and archival records (cases that are beyond regular retention guidelines). Records with lower RTO values, such as those related to current cases, will receive higher priority for backup and restoration. Records with higher RTO values, such as archival records, will have lower priority for backup and restoration.

B. Document backup systems and frequency of backups. Security and reliability of backups is a key element of successful disaster recovery. Software and hardware for this task should be identified and maintained in good condition and up to date. Many options are available for backing up data (see Appendix A).

8. Document data recovery procedures

A. Define priorities for data recovery.

B. Define the times available for recovery, accounting for decision-making time as well as actual data recovery time. For example, if recovery from a tape backup will require 3 hours and your RTO for that data type is 4 hours, that gives you 1 hour to weigh the situation and decide how to proceed.

C. Develop step-by-step procedures for retrieving data from backup sources, outlining steps for different types of data and different levels of loss. Situations may range from those where only current data needs to be restored, to those that require re-installation of the entire operating system and all software, to those that require new hardware.

D. Outline steps needed to re-enter/re-create any data that was outside the scope of the most current backup (re-enter from paper copy, etc.)

E. Provide a feedback process for post-crisis evaluation of outcomes, so that you can fine-tune your plan for improved future response.

IV. Plan Implementation

Once the Disaster Recovery Plan is complete, consider the following:

- Obtain any necessary approvals for implementation and funding.
- Budget for and purchase any needed equipment, supplies, and services.
- Budget for and complete any needed training.
- A DRP is a living document, and it will need to be revisited periodically as systems and personnel change over time. Plan for regular updates to the plan.
- Store copies of the plan in a waterproof container in a safe, yet easily accessible location. Consider hard copy and electronic forms of storage (recommend .pdf or .txt files on CD-ROM for portability), as well as off-site storage. If the plan will be kept in a locked area, document who has access to the area, and plan access/control measures for keys and/or lock combinations.
- Be sure that all personnel have read the plan and understand their roles in potential recovery efforts.
- Plan for regular dress rehearsals of key elements of the plan.

Appendix A: Backup System Options

With increasing reliance on information technology and business-critical data, much emphasis is placed on protecting irreplaceable data. The current data protection market is characterized by rapidly changing needs that are driven by data growth, regulatory issues, and the growing importance of accessing data quickly. In addition, an ever-shrinking time frame for backing up data is burdening conventional tape backup technologies. An ultimate data protection solution may involve a multi-faceted approach, utilizing both in-house and off-site methods.

1. On-site Backups: These consist of some type of magnetic or optical media where software/configuration info and data are copied on a periodic basis. These media can provide a backbone of storage for daily backups, and will protect data in the event of hardware failure or system crash, but can be virtually useless in the face of a major disaster such as fire, flood, or theft unless they are reliably stored in a locked, water-proof, and fire-proof container and refreshed on a frequent basis. Removing the media to a remote location for safekeeping on a regular basis increases the value of these types of systems. Most of these systems may be used remotely as well, such as over a local network or the internet (see off-site backups).

System	Pros	Cons
Tape Drive	• Widely used	• Old technology • Uses proprietary software; files recoverable only with specific software • Easily erased by magnets or exposure to sunlight • User dependent • Time-intensive • Do not provide random access to data
CD/RW Drive	• Long shelf life • Easy to store • Not vulnerable to magnetic fields	• Easily scratched • Easily forgotten or misplaced • User dependent • Relatively limited capacity
DVD/RW Drive	• Long shelf life • Easy to store • Not vulnerable to magnetic fields • Larger capacity than CD-ROM	• Easily scratched • Easily forgotten or misplaced • User dependent
External Hard Drive	• Long shelf life • Large capacity • Easy to store • Can be stored off-site	• More care needed than tapes or CD/DVDs • Easily compromised by exposure to magnetic fields • User dependent

Appendix A: Backup System Options, cont'd.

2. Off-site backups:

   A. Sneaker-net: A simple and inexpensive way to turn an on-site system into an off-site system is simply by carrying backup media to a safe remote location, such as a safe or bank security deposit box, on a regular basis. The drawbacks are:

      - The process is user dependent (may not be completed reliably)
      - Data may be vulnerable to loss or security breach while in transit
      - Accessibility may be limited (to bank hours, or, for example, if the data is stored in a personal safe)

   B. Remote backups: The increased accessibility of high-speed internet access makes it feasible to perform internet-based backups, such as electronic tape vaulting, on a regular basis. Commercial services or leased domains, such as nmmunicourts.org, can provide data storage at minimal cost. The drawbacks are:

      - Dependent on having an internet connection
      - May be software-dependent
      - May be a security risk
      - Data may be lost if the remote server suffers a disaster

3. Remote Data Centers: Cold site, warm site, and hot site facilities are different types of remote locations where a data center can be re-established in the event of a disaster. The following levels are commonly used:

   A. Cold Site: A cold site is a remote location that only provides the facility where data operations can be re-established in the event of a disaster. It includes neither equipment nor backed-up data, but does have power and communications capabilities. Significant time and effort would be needed to restore computing capacity, but a cold site incurs minimal cost. A cold site could be anywhere from an appropriately configured spare room in a community center to a leased facility.

   B. Warm Site: A warm site is a remote location similar to a cold site, but it is stocked with computer equipment. The hardware will be similar to, or at least compatible with, that of the original site, but it will not contain copies of software and data. Software and data will be retrieved from a separate backup system when they are needed.

   C. Hot Site: A hot site is a duplicate of the original site, with full computer systems as well as near-complete backups of user data. Replication or mirroring systems ensure that there will be little or no loss of data following a disaster, and that the business can perform a seamless transfer of operations. Hot sites may also be used to reduce downtime caused by developmental testing and maintenance. This type of site is expensive to operate, as it is basically a redundant data center. They are typically used only by businesses such as stock exchanges and financial institutions who must maintain real-time data.

Appendix A: Backup System Options, cont'd.

4. Additional Storage Options: Replication and mirroring technologies, as well as storage area networks (SANs) can provide near real-time access to lost data by automatically duplicating systems and data. When used remotely, they provide the added advantage of geographical diversity. They can range from simple (relatively inexpensive) to complex (high cost), but are typically used by organizations that require very high availability of data (near-zero values for RPO and RTO) and that have IT staff to design and maintain the system.

5. Comprehensive Solutions: Many companies offer services specializing in business continuity planning and off-site data protection, including some that offer mobile recovery service. An internet search can provide a current listing of these type of companies.

6. Backup Software: Many software applications can help with backups, such as:

    - Windows XP Pro
    - Symantec Backup Executive
    - Acronis True Image
    - Norton Ghost

Appendix B: Data Protection Measures

- Keep accurate and up-to-date records of equipment configurations, documentation, and software licenses.

- Perform regular comprehensive data backups. For most New Mexico municipal courts, this should occur at least weekly. Some larger courts may prefer daily backups.

- Send backups off-site; to facilitate recovery, include software as well as data.

- Identify early interventions that could help mitigate damage to systems and data for various scenarios.

- Use surge protectors to minimize the effect of power surges on electronic equipment.

- Use Uninterruptible Power Supplies (UPS) and/or a backup generator to mitigate effects of temporary power loss

- Expand use of fire prevention technology: linked alarms, accessible extinguishers, remote monitoring.

- Use and regularly update filtering and anti-virus software, and other security measures.

- Protect passwords and otherwise control access to information systems. Provide for immediate revisions to passwords if they are compromised.

- Store data and software backups, along with software licensing documents, in a locked, fireproof safe with controlled access.

- Design and/or adjust information systems to make data recovery easier. Purchase new systems with an eye toward ease of backup and recovery operations.

- Identify storage methods for archival materials that may be separate from current business data.

- Regardless of the type of backup system in use, a comprehensive backup strategy will include operating system and configuration data (such as a Windows XP system recovery disk) as well as software applications and data.

- Maintaining logical integrity between data and applications that may be interdependent is not a trivial matter. The court may consider the use of applications that have recovery and/or off-site backup built in to their capabilities.

Appendix C: Communication Measures for Municipal Courts

- Home and cellular phones: maintain a list of home and alternate (i.e., cellular) phones for court personnel as well as support personnel such as Municipal Court Automation staff, contractors, and software providers.

- Email: maintain a list of all available email addresses for all personnel, including backup service in an offsite account. The nmmunicourts.org domain is an existing option for off-site email service for municipal courts.

- Client contact information: maintain current lists list of home, work, and cellular phone numbers, as well as physical and email addresses for all plaintiffs, defendants, witnesses, and attorneys.

- Maintain current contact information for others who may need to be notified of an emergency, such as local law enforcement, correctional facilities, and municipal offices.

The following is an example of the type of document that can be used to document responsibilities and contact information:

Disaster Response Team Contact Information						
Position	Name	Title	Office Phone	Home phone (confidential)	Cell phone (confidential)	Email addresses/ physical location
Team Leader		Presiding Judge				
Assistant Team Leader		Court Administrator				
2nd Assistant Team Leader		Court Clerk				
IT Recovery Coordinator		Information Systems Manager				
Evacuation Coordinator		Safety Officer				
Law enforcement		Marshall				

Appendix D: General Considerations for Disaster Planning

- Develop staff support systems
    - During a disaster, employees may be asked to work longer hours under more stressful conditions. In a community-wide disaster, they may also have over-riding concerns for family and personal property. Consider support systems to alleviate some of these stresses.
    - Develop contingency plans for Human Resources and Payroll systems so that employees will not have added worries about interruption of payroll or benefits.
    - Staff may need to multitask during the disaster recovery process, so every staff member needs to understand the process. It is critical to not have a single person assigned to, and capable of, any given task, as that person may not be available to perform it.
- Address any special needs related to evacuation and relocation of court personnel and accessibility issues for personnel and the public.
- Appoint a responsible individual and establish procedures to protect financial resources, including checkbooks, debit and credit cards, and cash.
- Budget for incidental expenses related to recovery efforts.
- Coordinate with other municipal offices to share facilities on a temporary basis if offices and courtrooms are rendered unusable. Think about long-term relocation possibilities as well.
- Maintain adequate levels of insurance and review policies yearly. Even though many policies will not cover natural disasters or "acts of God," you may be able to request a rider for unusual situations (such as flood insurance) or equipment that exceeds the standard value of the policy.

Appendix E: References and Further Reading

Disaster Recovery; Wikipedia
http://en.wikipedia.org/wiki/Disaster_recovery#Technology

Cummings, E., Haag, S., & McCubbrey D. (2005). Management Information Systems for the Information Age. McGraw-Hill Ryerson Higher Education

City of St. Joseph, MO Disaster Recovery Plan; City of St. Joseph Department of Technology and Communication Services
http://www.ci.st-joseph.mo.us/tcs/DisasterRecoveryPlan.pdf

Disaster Recovery Planning for Courts, A Guide to Business Continuity; National Center for State Courts
http://www.ncsconline.org/WC/Publications/KIS_BusDisRcvyPlanCts.pdf

Emergency Preparedness in the State Courts; National Center for State Courts
http://www.ncsconline.org/WC/Publications//Trends/2006/TopTen/KIS_CtSecu_Trends06TopTen.pdf

Maryland Continuity of Operations Planning Manual; Maryland Emergency Management Agency
http://www.umaryland.edu/healthsecurity/navigation/Version%202%20Final%20Coop%20Manual.pdf

The Technology of Disaster Recovery; Symantec Veritas Architect Network
http://www.veritas.com/van/articles/3943.jsp

Storage Area Network; Wikipedia
http://en.wikipedia.org/wiki/Storage_area_network